Security concerns at DOH

HIPAA requires data and computer security

By Joshua Schmidt
Information Systems Security Administrator
DOH

This is the third in a series of *Sentinel* articles to discuss aspects of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA).

HIPAA is a response to growing computerization in health care, including the rapid growth of electronic transfers of health information. The act addresses concerns about the confidentiality of the health care information that is part of the growing universe of electronic commerce.

The most far-reaching HIPAA regulations are the Security and Electronic Signature Standards. The security standards require any health plan, health care clearinghouse, or health care provider that maintains or transmits electronic health information to assess its security risks and needs. The organization must then devise, implement, and maintain appropriate security measures. Anyone receiving health information from them must comply with the same security standards.

It is not yet clear what areas of the Department of Health are directly required to comply with the standards, but all program areas will be at least indirectly affected. Because we are all part of the same organization with interconnected systems, all parts of the department must comply with the security regulations, which cover the following areas:

Administrative procedures: Procedures to protect data such as data sharing agreements and security training.

Physical safeguards: Protection of the computers from fire and other natural and environmental hazards, as well as from theft and unauthorized access.

Technical safeguards: Processes to protect data, monitor individual access to information, and prevent unauthorized access to data while it is being transmitted.

Once the final security rules have been published, this December, we will have 2 years to comply with the standards. Each requirement has implementation features that must be met to demonstrate compliance to federal auditors and business partners. Organizations that do not fully comply could face severe penalties.

We have much to do in a short time, and we need commitment from everyone in the agency to get it done. Current activities include:

Administrative Procedures

- Instituting agency policies for employee responsibilities with confidential data.
- Directing the development of confidentiality policies and procedures at the division and office/program level.
- Requiring confidentiality and security training.
- Developing standard data sharing agreements.

- Working with the Community Health Information Technology Alliance (CHITA) on establishing consistent and appropriate privacy principles and practices for public and private organizations.

Physical Safeguards

- Planning for physical security in the design of the proposed new building in Olympia.
- Increasing the use of card keys for access to current facilities (1102 Quince Street, Public Health Laboratories).
- Establishing reception desks to monitor public access to department buildings.

Technical Security

- Working with the Department of Information Systems and other agencies to implement encryption and electronic signatures for the state.
- Working with CHITA on pilot projects to create secure, standardized methods for sharing information across the Internet.
- Boosting computer network security by adding a virtual guard at the entrance to our network (a firewall), and setting up a more secure method for accessing our systems from home or other external sites.

Future articles will explain computer security issues and provide guidelines for keeping your systems secure.